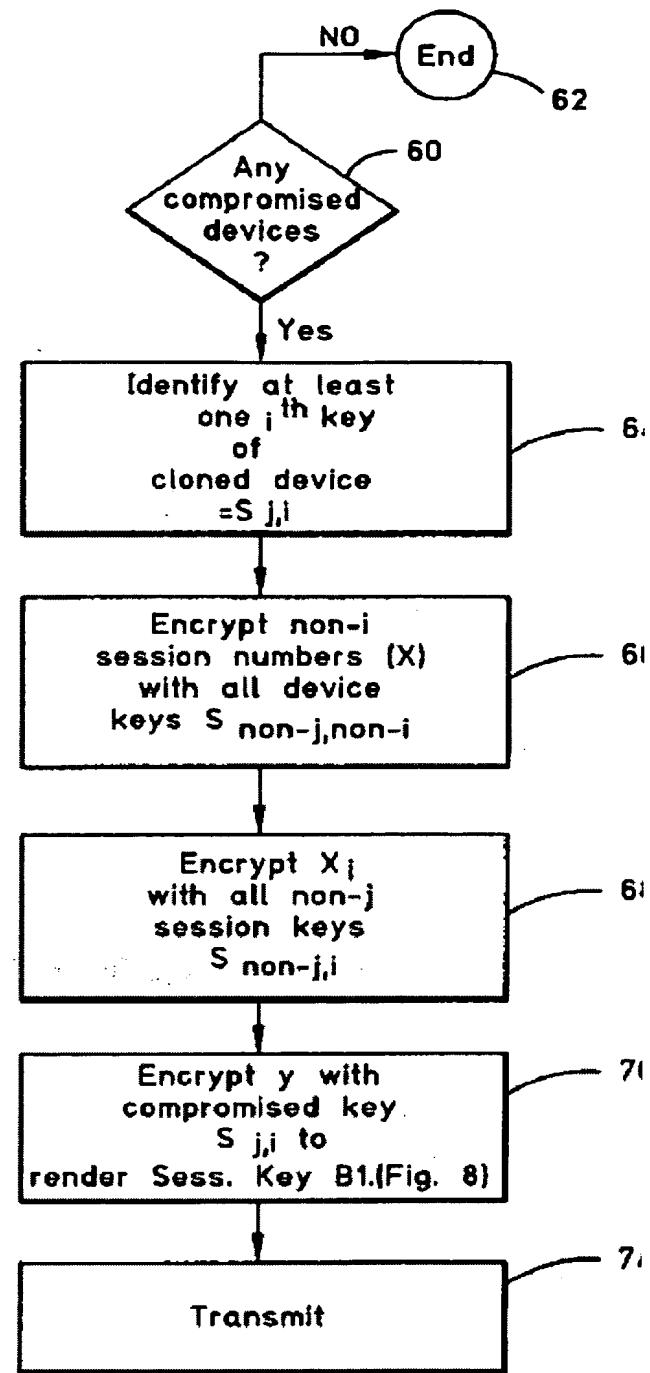


SYSTEM AND METHOD FOR ENCRYPTING BROADCAST PROGRAM**Publication number:** JP2000031922**Also published as:****Publication date:** 2000-01-28 US6118873 (A)**Inventor:** JEFFREY BRUCE LOTSPEACH; KEVIN SNOW
MACURLEY**Applicant:** IBM**Classification:****- international:** H04L9/00; H04L9/08; H04N7/167; H04L9/00;
H04L9/08; H04N7/167; (IPC1-7): H04H1/00; H04L9/08;
H04N7/167**- european:** H04L9/00; H04L9/08; H04N7/167D**Application number:** JP19990107957 19990415**Priority number(s):** US19980065938 19980424**Report a data error here****Abstract of JP2000031922**

PROBLEM TO BE SOLVED: To provide a transmission method of a digital program with security to in-home digital devices even when parts of the devices are not allowed by a digital broadcast system. **SOLUTION:** The system is provided with a matrix whose elements are device keys $S_{i,j}$, where ' i ' denotes a key index variable indicating a position in the matrix in terms of a key-dimension and ' j ' shows a set index variable depicting a position in the matrix in terms of a set-dimension. This matrix is used to assign plural device keys each assigned to only one in-home device depending on each key index variable ' i '. In order to generate a session key for a broadcast program, all the device keys $S_{i,j}$, are used to encrypt session numbers x_i and to generate a session key block that is used to generate the session key that decodes the program by each in-home device. In the case that any of the devices is a device not permitted by the digital broadcast system a dummy number is assigned to at least a session number 50 that the dummy number is encrypted by a corresponding key for the device not permitted by the system and the resulting decoded session key is not useful to decode the program key.

This Page Blank (uspto)



Data supplied from the **esp@cenet** database - Worldwide

This Page Blank (uspto)

特開2000-31922

(P2000-31922A)

(43) 公開日 平成12年1月28日(2000.1.28)

(51) Int. C.I. 7
 H 04 H 1/00
 H 04 L 9/08
 H 04 N 7/167

識別記号

F I
 H 04 H 1/00
 H 04 L 9/00
 H 04 N 7/167

F
 6 0 1 E
 6 0 1 A
 Z

マーク(参考)

審査請求 有 請求項の数 3 6 O L

(全 23 頁)

(21) 出願番号 特願平11-107957
 (22) 出願日 平成11年4月15日(1999.4.15)
 (31) 優先権主張番号 09/065938
 (32) 優先日 平成10年4月24日(1998.4.24)
 (33) 優先権主張国 米国(US)

(71) 出願人 390009531
 インターナショナル・ビジネス・マシーンズ・コーポレイション
 INTERNATIONAL BUSIN
 ESS MACHINES CORPO
 RATION
 アメリカ合衆国10504、ニューヨーク州
 アーモンク (番地なし)
 (72) 発明者 ジェフリー・ブルース・ロツツピーチ
 アメリカ合衆国95123 カリフォルニア州
 サンノゼ フットヒル・ドライブ 992
 (74) 代理人 100086243
 弁理士 坂口 博 (外1名)

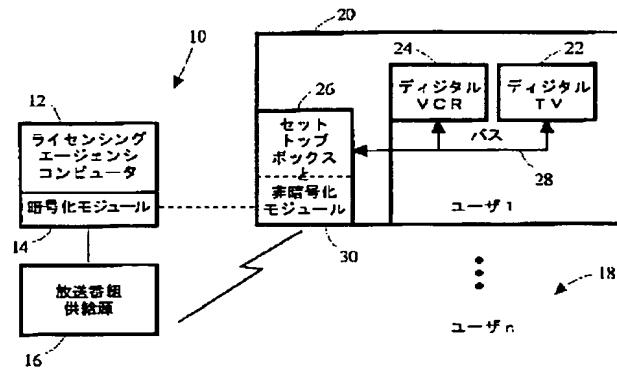
最終頁に続く

(54) 【発明の名称】放送番組を暗号化するためのシステムおよび方法

(57) 【要約】

【課題】 デジタル放送システムが、装置の一部が許可されないものである時でも家庭内ディジタル装置へのディジタル番組の保護された送信を提供する。

【解決手段】 装置鍵 S_{ij} の行列を設ける。ここで、「 i 」は、行列の鍵次元での位置を示す鍵インデックス変数であり、「 j 」は、行列の集合次元での位置を示す集合インデックス変数である。家庭内装置のそれぞれには、鍵インデックス変数「 i 」ごとに1つの装置鍵だけが装置に割り当てられる形で、この行列からの複数の装置鍵が割り当てられる。放送番組用のセッション鍵を生成するために、すべての装置鍵 S_{ij} を用いてセッション番号 x_{ij} を暗号化して、家庭内装置によって非暗号化され、番組を非暗号化するためのセッション鍵の生成に使用されるセッション鍵ブロックを生成する。装置のうちの1つが暗号漏洩された装置である場合には、少なくとも1つのセッション番号を、対応する暗号漏洩された装置鍵によって暗号化され、非暗号化され、結果のセッション鍵が番組の非暗号化に有用でなくなるダミー番号にする。



【特許請求の範囲】

【請求項1】装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵をそれぞれが含む複数のユーザ装置と、

セッション鍵ブロックを作るために装置鍵の前記集合を用いて複数のセッション番号を暗号化するための少なくとも1つのセッション鍵ブロック・ジェネレータであって、前記装置のうちの少なくとも1つが暗号漏洩された装置鍵を定義する暗号漏洩された装置であると判定された時に前記セッション番号のうちの少なくとも1つがダミー番号になり、前記ダミー番号が少なくとも1つの暗号漏洩された装置鍵によって暗号化され、前記セッション鍵ブロックが番組の非暗号化に使用するために送信される、前記少なくとも1つのセッション鍵ブロック・ジェネレータと、

各ユーザ装置にアクセスでき、前記セッション鍵ブロックおよび前記装置のそれぞれの前記装置鍵に基づいてセッション鍵を判定するために前記装置の前記装置鍵にアクセスする非暗号化モジュールであって、前記セッション鍵が、前記装置が前記セッション鍵の生成に前記ダミー番号を使用しない限り、前記番組を非暗号化するためにユーザ装置によって使用可能である、前記非暗号化モジュールとを含む、1つまたは複数の放送番組を暗号化するためのシステム。

【請求項2】装置鍵の前記集合が、鍵次元および集合次元を含む少なくとも2次元の行列によって表され、前記鍵次元が、鍵インデックス変数「i」によってそれぞれが表される「N」個の鍵位置を表し、前記集合次元が、集合インデックス変数「j」によってそれぞれが表される「M」個の集合を表し、各装置鍵をS_{1,1}によって表すことができる、請求項1のシステム。

【請求項3】ある装置の2つの装置鍵のいずれもが、互いに同一の鍵インデックス変数「i」を有しない、請求項2のシステム。

【請求項4】各セッション番号をx_{1,1}によって表すことができるよう、鍵インデックス変数「i」ごとにそれぞれのセッション番号が設けられ、各セッション番号x_{i,1}が、前記セッション鍵ブロックを作るために第i鍵次元の装置鍵によってのみ暗号化される、請求項3のシステム。

【請求項5】暗号漏洩された装置鍵を有しないすべての装置が、少なくとも第1セッション鍵を生成し、暗号漏洩された装置鍵を有するすべての装置が、少なくとも第2セッション鍵を生成し、第1セッション鍵だけが前記番組の非暗号化に有用になるように、各装置が、前記第iセッション番号を非暗号化するためにそれぞれの第i装置鍵S_{1,1}を使用する、請求項4のシステム。

【請求項6】前記第1セッション鍵を生成する装置が、少なくとも第1プールを定義し、前記第2セッション鍵を生成する装置が、少なくとも第2プールを定義し、前

記システムがさらに、前記第1プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に前記第1プール内の前記装置に、前記装置が新しい装置鍵を生成するために操作する更新データを送信するためのコンピュータ可読コード手段を含む、請求項5のシステム。

【請求項7】前記第2セッション鍵を生成する装置が、少なくとも第2プールを定義し、前記システムがさらに、前記第2プール内のすべての装置が暗号漏洩された

10 装置であるかどうかを判定し、そうでない場合に前記第2プール内の装置に新しいセッション鍵を生成させるためのコンピュータ可読コード手段を含む、請求項5のシステム。

【請求項8】暗号漏洩されない装置の第1集合が、第1プールを定義し、暗号漏洩されない装置の第2集合が、第3プールを定義し、前記第1プールおよび前記第3プールのそれぞれが、暗号漏洩された装置を含まず、前記システムがさらに、前記第1プール内の装置に、そのセッション鍵を前記第3プール内の装置の前記セッション鍵によって置換させるためのコンピュータ可読コード手段を含む、請求項5のシステム。

【請求項9】ディジタル番組を放送するためにこれを暗号化するためのコンピュータ使用可能コード手段を有するコンピュータ使用可能媒体を含むデータ記憶装置を具備するコンピュータにおいて、前記コンピュータ使用可能コード手段が、

iが1とNを含む1からNまでの整数であり、jが1とMを含む1からMまでの整数であり、「i」が装置鍵S_{1,1}の行列の鍵次元での位置を示す鍵次元インデックス30 変数であり、「j」が前記行列の集合次元での位置を示す集合インデックス変数であり、「N」が鍵のM個の集合のそれぞれの装置鍵の個数であるものとして、前記装置鍵S_{1,1}の行列にアクセスするためのコンピュータ可読コード手段と、

鍵インデックス変数「i」ごとに各ディジタル・ビデオ装置に1つの装置鍵だけが割り当てられるように、複数の前記ディジタル・ビデオ装置に装置鍵の前記行列からそれぞれの複数の装置鍵を割り当てるためのコンピュータ可読コード手段と、

40 iが1とNを含む1からNまでの整数であるものとして、各セッション番号x_{i,1}がそれぞれの鍵インデックス変数「i」に対応するように複数の前記セッション番号x_{i,1}を生成するためのコンピュータ可読コード手段と、「j」が1とMを含む1からMまでの整数であるものとして、セッション鍵ブロックを生成するために、すべての装置鍵S_{1,1}を用いて各セッション番号x_{i,1}を暗号化するためのコンピュータ可読コード手段とを含む、コンピュータ。

【請求項10】前記ディジタル・ビデオ装置のうちの1つまたは複数が暗号漏洩された装置であるかどうかを判

50

定するためのコンピュータ可読コード手段と、

前記暗号漏洩された装置の少なくとも1つの暗号漏洩された装置鍵によって暗号化されるダミー番号として、前記セッション番号のうちの少なくとも1つを作るためのコンピュータ可読コード手段とをさらに含む、請求項9のコンピュータ。

【請求項11】第1デジタル・ビデオ装置が、第1セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第1デジタル・ビデオ装置が、少なくとも第1プールを定義し、第2デジタル・ビデオ装置が、第2セッション鍵を生成するために前記セッション鍵のうちの少なくとも一部を非暗号化し、前記第2デジタル・ビデオ装置が、少なくとも第2プールを定義し、前記コンピュータがさらに、

前記第1プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に前記第1プール内の前記デジタル・ビデオ装置に、前記デジタル・ビデオ装置が新しい装置鍵を生成するために操作する更新データを送信するためのコンピュータ可読コード手段を含む、請求項10のコンピュータ。

【請求項12】第2デジタル・ビデオ装置が、第2セッション鍵を生成するために前記セッション鍵ブロックの少なくとも一部を非暗号化し、前記第2デジタル・ビデオ装置が、少なくとも第2プールを定義し、前記コンピュータがさらに、前記第2プール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合に前記第2プール内の装置に新しいセッション鍵を生成させるためのコンピュータ可読コード手段を含む、請求項10のコンピュータ。

【請求項13】暗号漏洩されない装置の第1集合が、第1プールを定義し、暗号漏洩されない装置の第2集合が、第3プールを定義し、前記第1プールおよび前記第3プールのそれぞれが、暗号漏洩された装置を含まず、前記コンピュータがさらに、前記第1プール内の装置に、そのセッション鍵を前記第3プール内の前記装置の前記セッション鍵によって置換させるためのコンピュータ可読コード手段を含む、請求項10のコンピュータ。

【請求項14】前記デジタル・ビデオ装置と組み合わされた、請求項9のコンピュータ。

【請求項15】iが1とNを含む1からNまでの整数であり、jが1とMを含む1からMまでの整数であり、「N」が鍵のM個の集合のそれぞれの装置鍵の数であるものとして、それぞれが「j」装置鍵S_jによって暗号化されるセッション番号x_jを含み、少なくとも次元「i」および「j」を有する行列によって表現できるセッション鍵ブロックを受信するためのコンピュータ可読コード手段と、

変数「i」ごとに1つだけデジタル・ビデオ装置に割

り当てられる複数の局所装置鍵にアクセスするためのコンピュータ可読コード手段と、

前記局所装置鍵を使用して前記セッション鍵ブロックからのセッション鍵を非暗号化するためのコンピュータ可読コード手段とを含む、少なくとも1つのデジタル番組を受信し、提示するために構成された前記デジタル・ビデオ装置のための非暗号化モジュール。

【請求項16】さらに、前記デジタル・ビデオ装置が暗号漏洩された装置鍵を有しない場合に、前記デジタル・ビデオ装置が第1セッション鍵を生成し、前記デ

ジタル・ビデオ装置が1つまたは複数の暗号漏洩された装置鍵を有する場合に、前記デジタル・ビデオ装置が第2セッション鍵を生成し、前記第1セッション鍵だけが前記デジタル・ビデオ番組の非暗号化に有用になるよう、第iセッション番号を非暗号化するためにそれぞれの第i局所装置鍵を使用するためのコンピュータ可読コード手段を含む、請求項15のモジュール。

【請求項17】さらに、更新データを受信するためのコンピュータ可読コード手段を含み、前記モジュールが、

1つまたは複数の新しい局所装置鍵を生成するために前記更新データを操作するために1つまたは複数の前記局所装置鍵を使用する、請求項16のモジュール。

【請求項18】さらに、放送メッセージに応答して、前記セッション鍵を他の装置のセッション鍵によって置換するためのコンピュータ可読コード手段を含む、請求項17のモジュール。

【請求項19】装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵を複数のユーザ装置に供給するステップと、

30 セッション鍵ブロックを作るために装置鍵の前記集合を用いて複数のセッション番号を暗号化する少なくとも1つのセッション鍵ブロック・ジェネレータを生成するステップと、

前記ユーザ装置のうちの少なくとも1つが、暗号漏洩された装置鍵を定義する暗号漏洩された装置であることが判定された時に、前記セッション番号のうちの少なくとも1つがダミー番号になるように定義するステップと、暗号漏洩された装置鍵を用いて前記ダミー番号を暗号化するステップと、

40 1つまたは複数の放送番組の非暗号化に使用するために前記セッション鍵ブロックを送信するステップと、前記ユーザ装置がセッション鍵の生成に前記ダミー番号を使用しない限り、前記番組を非暗号化するためにユーザ装置によって使用可能な前記セッション鍵を、前記セッション鍵ブロックおよび前記ユーザ装置のそれぞれの前記装置鍵に基づいて判定するために各ユーザ装置の前記装置鍵にアクセスするステップとを含む、前記1つまたは複数の放送番組の保護された送信のためのコンピュータ実施される方法。

50 【請求項20】装置鍵の前記集合が、鍵次元および集合

次元を含む少なくとも2次元の行列によって表現可能であり、前記鍵次元が、鍵インデックス変数「i」によってそれが表される「N」個の鍵位置を表し、前記集合次元が、集合インデックス変数「j」によってそれが表される「M」個の集合を表し、各装置鍵をS_{..}によって表すことができるようになっている、請求項19の方法。

【請求項21】あるユーザ装置の2つの装置鍵のどれもが、互いに同一の鍵インデックス変数「i」を有しない、請求項20の方法。

【請求項22】各セッション番号をx_{..}によって表すことができるよう、鍵インデックス番号「i」ごとにそれぞれのセッション番号を供給するステップと、前記セッション鍵ブロックを作るために、第i鍵次元の装置鍵だけを用いて各セッション番号x_{..}を暗号化するステップとを含む、請求項21の方法。

【請求項23】前記暗号漏洩された装置鍵を有しないすべてのユーザ装置が、少なくとも第1セッション鍵を生成し、前記暗号漏洩された装置鍵を有するすべてのユーザ装置が、少なくとも第2セッション鍵を生成し、前記第1セッション鍵だけが、前記番組の非暗号化に有用になるように、各ユーザ装置が、第iセッション番号を非暗号化するためにそれぞれの第i装置鍵S_{..}を使用する、請求項22の方法。

【請求項24】前記第1セッション鍵を生成するユーザ装置が、少なくとも第1プールを定義し、前記第2セッション鍵を生成するユーザ装置が、少なくとも第2プールを定義し、前記方法がさらに、

前記第1プール内のすべてのユーザ装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に、前記第1プール内の前記ユーザ装置に、新しい装置鍵を生成するために前記ユーザ装置が操作する更新データを送信するステップを含む、請求項23の方法。

【請求項25】前記第2セッション鍵を生成するユーザ装置が、少なくとも第2プールを定義し、前記方法がさらに、

前記第2プール内のすべてのユーザ装置が、暗号漏洩された装置であるかどうかを判定し、そうでない場合に、前記第2プール内のユーザ装置に新しいセッション鍵を生成させるステップを含む、請求項23の方法。

【請求項26】暗号漏洩されていない装置の第1集合が、第1プールを定義し、暗号漏洩されていない装置の第2集合が、第3プールを定義し、前記第1プールおよび前記第3プールのそれぞれが、暗号漏洩された装置を含まず、前記方法がさらに、

前記第1プール内の装置に、前記第3プール内の前記装置の前記セッション鍵を用いてそれぞれのセッション鍵を置換させるステップを含む、請求項23の方法。

【請求項27】ディジタル処理装置によって読み取ることができるコンピュータ・プログラム記憶装置と、

デジタル番組の放送のためにこれを暗号化するための方法ステップを実行するために前記ディジタル処理装置によって実行可能な命令を含む、前記プログラム記憶装置上のプログラム手段とを含み、前記方法ステップが、

iが1とNを含む1からNまでの整数であり、jが1とMを含む1からMまでの整数であり、「i」が装置鍵S_{..}の行列の鍵次元での位置を示す鍵インデックス変数であり、「j」が前記行列の集合次元での位置を示す集合インデックス変数であり、「N」が鍵のM個の集合の

10 それぞれの装置鍵の数であるものとして、前記装置鍵S_{..}の行列にアクセスするステップと、

鍵インデックス変数「i」ごとに各ディジタル・ビデオ装置に1つの装置鍵だけが割り当てる形で、複数の前記ディジタル・ビデオ装置に、前記装置鍵の行列から複数の装置鍵を割り当てるステップと、

iが1とNを含む1からNまでの整数であるものとして、それぞれが鍵インデックス変数「i」に対応する複数のセッション番号x_{..}を生成するステップと、

jが1とMを含む1からMまでの整数であるものとして、セッション鍵ブロックを生成するために、すべての装置鍵S_{..}を用いて各セッション番号x_{..}を暗号化するステップとを含む、コンピュータ・プログラム装置。

【請求項28】前記方法ステップがさらに、前記ディジタル・ビデオ装置のうちの1つまたは複数が暗号漏洩された装置であるかどうかを判定するステップと、

前記暗号漏洩された装置の少なくとも1つの暗号漏洩された装置鍵によって暗号化されるダミー番号として、前記セッション番号のうちの少なくとも1つを作るステップとを含む、請求項27のコンピュータ・プログラム装置。

【請求項29】第1ディジタル・ビデオ装置が、第1セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第1ディジタル・ビデオ装置が、少なくとも第1プールを定義し、

第2ディジタル・ビデオ装置が、第2セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第2ディジタル・ビデオ装置が、少なくとも第2プールを定義し、前記方法ステップがさらに、

前記第1プール内のすべてのディジタル・ビデオ装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に、新しい装置鍵を生成するために前記第1プール内の前記ディジタル・ビデオ装置が操作する更新データを前記第1プール内の前記ディジタル・ビデオ装置に送信するステップを含む、請求項28のコンピュータ・プログラム装置。

【請求項30】第2ディジタル・ビデオ装置が、第2セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第2ディジ

タル・ビデオ装置が、少なくとも第2プールを定義し、前記方法ステップがさらに、前記第2プール内のすべてのディジタル・ビデオ装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合は、前記第2プール内のディジタル・ビデオ装置に新しいセッション鍵を生成させるステップを含む、請求項28のコンピュータ・プログラム装置。

【請求項31】暗号漏洩されない装置の第1集合が、第1プールを定義し、暗号漏洩されない装置の第2集合が、第3プールを定義し、前記第1プールおよび前記第3プールのそれぞれが、暗号漏洩された装置を含まず、前記方法ステップがさらに、前記第1プール内の装置に、前記第3プール内の前記装置のセッション鍵を用いてそのセッション鍵を置換させるステップを含む、請求項28のコンピュータ・プログラム装置。

【請求項32】前記ディジタル・ビデオ装置と組み合わされた、請求項27のコンピュータ・プログラム装置。

【請求項33】ディジタル処理装置によって読み取ることができるコンピュータ・プログラム記憶装置と、ディジタル・ビデオ装置に少なくとも1つのディジタル番組を受信させ、提示させるための方法ステップを実行するために前記ディジタル処理装置によって実行可能な命令を含む、前記コンピュータ・プログラム記憶装置上のプログラム手段とを含み、前記方法ステップが、
iが1とNを含む1からNまでの整数であり、jが1とMを含む1からMまでの整数であり、「N」が鍵のM個の集合のそれぞれの装置鍵の数であるものとして、各セッション番号x_iが第j装置鍵S_jによって暗号化される暗号化されたセッション番号x_iを含む、少なくとも次元「i」および「j」を有する行列によって表すことのできるセッション鍵ブロックを受信するステップと、前記ディジタル・ビデオ装置に変数「i」ごとに1つだけ割り当てられる複数の局所装置鍵にアクセスするステップと、

前記局所装置鍵を使用して前記セッション鍵ブロックからのセッション鍵を非暗号化するステップとを含む、コンピュータ・プログラム装置。

【請求項34】前記方法ステップがさらに、前記ディジタル・ビデオ装置が暗号漏洩された装置鍵を有しない場合には、前記ディジタル・ビデオ装置が第1セッション鍵を生成し、前記ディジタル・ビデオ装置が1つまたは複数の暗号漏洩された装置鍵を有する場合には、前記ディジタル・ビデオ装置が第2セッション鍵を生成し、前記第1セッション鍵だけが前記ディジタル番組の非暗号化に有用になるように、第iセッション番号を非暗号化するためにそれぞれの第i局所装置鍵を使用するステップを含む、請求項33のコンピュータ・プログラム装置。

【請求項35】前記方法ステップがさらに、

更新データを受信するステップと、

1つまたは複数の新しい局所装置鍵を生成するために、前記更新データを操作するのに1つまたは複数の前記局所装置鍵を使用するステップとを含む、請求項34のコンピュータ・プログラム装置。

【請求項36】前記方法ステップがさらに、放送メッセージに応答して、前記セッション鍵を他の装置のセッション鍵によって置換するステップを含む、請求項35のコンピュータ・プログラム装置。

10 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、全般的にはデータ暗号化に関し、具体的には、許可されていないクローン受信器が番組を簡単に非暗号化できないようにする、放送番組の暗号化に関する。

【0002】

【従来の技術】たとえば衛星またはケーブルによるペイ・パー・ビュー(pay-per-view)放送番組の、支払いを行わない顧客による許可されていない視聴およびコピーを防ぐために、そのような番組は、通常は暗号化される。許可された顧客には、その内部の非暗号化アルゴリズムに従って番組を非暗号化する、いわゆる「セット・トップ・ボックス」が与えられる。受信した番組に対する料金を許可された顧客に確実に請求するために、さまざまな課金方式が、セット・トップ・ボックスまたは他の顧客識別に結び付けられている。

【0003】支払いを行わない多数の顧客に対するアクセスの阻止には有効であるが、このようなセット・トップ・ボックスは、比較的洗練されたクローニング技術を

30 使用してクローンを作成し、販売することができ、これを購入した者は、そのクローンを使用して、本来はペイ・パー・ビューである番組を無料で視聴し、コピーすることができる。単独のクローン・ボックスがたまたま発見される可能性はあるが、大半は使用者の家庭で検出されないままになり、放送局の収入の損失につながる。

【0004】この収入の損失は、ディジタル・コピーが完全なコピーであるから、特に家庭用ディジタル・ビデオ装置の発達に伴って、大きな問題になりつつある。実際、ディジタル・ビデオの発達は、「Firewire

40 e」または「IEEE 1394」と称する新しいディジタル・バス標準規格の導入をもたらした。この標準規格は、ユーザのディジタル・テレビジョン、ディジタル・ビデオ・カセット・レコーダ(VCR)、Digital Versatile Disk(DVD)プレイヤーおよびセット・トップ・ボックスの間の相互接続を標準化するために提案されたものである。

【0005】数百万台のセット・トップ・ボックスが同一の非暗号化アルゴリズム鍵を使用する可能性があるので、許可された装置のそれぞれに新しい非暗号化アルゴリズム鍵を個別に再プログラムすることは実現可能では

9
ない。実際、数百万台のペイ・パー・ビュー番組の家庭内非暗号化受信器を再プログラムするための実現可能な唯一の方法は、新しい暗号化アルゴリズム鍵を送ることであるが、許可されないクローンも、その新しい鍵の放送を受信し、古典的な放送暗号化の難問すなわち、許可されないクローンから権利を剥奪しながら、許可された受信器に新しい非暗号化鍵を効果的に再プログラミングするにはどうするかという問題につながる。本発明は、この問題に対処する。

【0006】

【発明が解決しようとする課題】したがって、本発明の目的は、保護された番組放送のための暗号化システムを提供することである。本発明のもう1つの目的は、許可された家庭内デジタル・ビデオ装置に暗号化更新を放送できる暗号化システムを提供することである。本発明のもう1つの目的は、許可された家庭内デジタル・ビデオ装置の暗号化アルゴリズムを更新できると同時に、既知の許可されない装置が効果的に更新されないようにする暗号化システムを提供することである。本発明のもう1つの目的は、使いやすくコスト効率のよい、保護された番組放送のための暗号化システムを提供することである。

【0007】

【課題を解決するための手段】1つまたは複数の放送番組を暗号化するためのシステムを開示する。このシステムには、複数のユーザ装置が含まれ、このユーザ装置のそれぞれに、装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵が含まれる。セッション鍵ブロック・ジェネレータが、装置鍵の集合を用いて複数のセッション番号を暗号化して、セッション鍵ブロックを作り、少なくとも1つの装置が暗号漏洩された装置鍵を定義する暗号漏洩された装置であると判定される時に、少なくとも1つのセッション番号をダミー番号にことができる。ダミー番号は、暗号漏洩された装置鍵によって暗号化され、その後、セッション鍵ブロックが、番組の非暗号化に使用するために送信される。各ユーザ装置にアクセスできる非暗号化モジュールは、その装置の装置鍵にアクセスして、セッション鍵ブロックとその装置のそれぞれの装置鍵とにに基づいてセッション鍵を決定することができる。装置が暗号漏洩された装置鍵を有しないならば、このセッション鍵を使用してユーザ装置が番組を非暗号化できるが、暗号漏洩された装置鍵を有する装置では、結果的にダミー番号が非暗号化され、これを使用してセッション鍵が生成される。

【0008】好ましい実施例では、装置鍵の集合を、鍵次元と集合次元を含む少なくとも2次元の行列によって表現できる。鍵次元では、それぞれが鍵インデックス変数「i」によって表される「N」個の鍵位置が表され、集合次元では、それぞれが集合インデックス変数「j」によって表される「M」個の集合が表され、各装置鍵を

表記 $S_{i,j}$ によって表すことができるようになってい
る。下で詳細を示す原理によれば、ある装置の2つの装置鍵が互いに同一の鍵インデックス変数「i」を有する
ことはない。

【0009】好ましい実施例では、各セッション番号を
 x_i によって表せるように、鍵インデックス変数「i」
ごとにそれぞれのセッション番号が提供される。各セッ
ション番号 x_i は、セッション鍵ブロックを作るため
に、第 i 鍵次元の装置鍵によってのみ暗号化される。さ

10 らに、各装置は、それぞれの第 i 装置鍵 $S_{i,j}$ を使用して
第 i セッション番号を非暗号化して、暗号漏洩された
装置鍵を有しないすべての装置が、少なくとも第1セッ
ション鍵を生成し、暗号漏洩された装置鍵を有するすべて
の装置が、少なくとも第2セッション鍵を生成し、第
1セッション鍵だけが番組の非暗号化に有用になる。

【0010】特に好ましい実施例では、第1セッション
鍵を生成する装置によって第1プールが定義され、第2
セッション鍵を生成する装置によって第2プールが定義
される。コンピュータ可読コード手段によって、第1プ

20 ルル内のすべての装置が暗号漏洩された装置でないかどうかを判定し、それらが暗号漏洩された装置でない場合
には、暗号化された更新データがすべての装置に送られる。第1プールの装置だけが、この更新データを非暗号
化でき、正しく操作することができる。これらの装置
は、更新データを操作して、新しい装置鍵を生成する。
さらに、コンピュータ可読コード手段によって、第2プ
ール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合には、第2プールの装置
に、異なる暗号漏洩された装置鍵を使用して新しいセッ
ション鍵を生成させる。

30 【0011】好ましい実施例のもう1つの特徴では、暗
号漏洩されていない装置の第1の集合によって第1プ
ールが定義され、暗号漏洩されていない装置の第2の集合
によって第2プールが定義され、第1プールと第2プ
ールのそれぞれに暗号漏洩された装置が含まれないように
なっている。このような状況で帯域幅を節約するため
に、コンピュータ可読コード手段によって、第1プール
の装置に、そのセッション鍵を第2プールの装置のセッ
ション鍵で置換させる。上で示したシステムの機能を実
行するコンピュータ実施される方法も開示される。

【0012】もう1つの態様では、本発明は、放送データを暗号化するために本明細書に記載の発明的ステップ
に従ってプログラミングされた汎用コンピュータであ
る。本発明は、デジタル処理装置によって使用され、
放送送信を暗号化するためにデジタル処理装置によ
つて実行できる命令のプログラムを具体的に実施する製
品（機械構成要素）として実施することもできる。本発
明は、デジタル処理装置に本明細書に記載の発明的方
法ステップを実行させるクリティカルな機械構成要素に
おいて実現される。

【0013】本発明によれば、方法ステップに、 i が1からNまで（両端を含む）の整数、 j が1からMまで（両端を含む）の整数として、装置鍵 $S_{i,j}$ の行列にアクセスするステップが含まれる。本発明の原理によれば、「 i 」は、この行列の鍵次元での位置を示す鍵インデックス変数であり、「 j 」は、行列の集合次元での位置を示す集合インデックス変数であり、「N」は、鍵の「M」個の集合のそれぞれに含まれる装置鍵の数である。装置鍵の行列からの複数の装置鍵のそれぞれに、複数のデジタル・ビデオ装置が割り当てられ、このデジタル・ビデオ装置のそれぞれに、鍵インデックス変数「 i 」ごとに1つの装置鍵だけが割り当てられる。さらに、複数のセッション番号 x_i （ $i = 1, \dots, N$ ）が生成され、セッション番号 x_i のそれぞれが、それぞれの鍵インデックス変数「 i 」に対応する。セッション番号 x_i のそれぞれを、すべての装置鍵 $S_{i,j}$ （ $j = 1, \dots, M$ ）を用いて暗号化して、セッション鍵ブロックを生成する。

【0014】もう1つの態様では、少なくとも1つのデジタル番組を受信し、提示するように構成された、デジタル・ビデオ装置のための非暗号化モジュールが開示される。このモジュールには、少なくとも次元「 i 」および「 j 」を有する行列によって表現されるセッション鍵ブロックを受信するためのコンピュータ可読コード手段が含まれる。セッション鍵ブロックには、暗号化されたセッション番号 x_i （ $i = 1, \dots, N$ ）が含まれ、セッション番号 x_i のそれぞれは、「 j 」装置鍵 $S_{i,j}$ （ $j = 1, \dots, M$ ）によって暗号化される。本明細書で使用する「N」は、鍵の「M」個の集合のそれぞれに含まれる装置鍵の数である。コンピュータ可読コード手段は、複数の局所装置鍵にアクセスするが、変数「 i 」に対して、ビデオ装置に1つの局所装置鍵だけが割り当てられることを理解されたい。また、コンピュータ可読コード手段には、局所装置鍵を使用してセッション鍵ブロックからセッション鍵を非暗号化するステップが含まれる。この非暗号化モジュールの機能を実行するコード手段を有するコンピュータ・プログラム製品も開示される。

【0015】

【発明の実施の形態】まず図1を参照すると、保護された番組放送のためのシステム10が示されている。「放送」とは、ケーブル、ワイヤまたは無線を介して多数のユーザに同時に番組を広く行き渡らせることを意味する。図示の特定のアーキテクチャでは、システム10に、ライセンシング・エージェンシ・コンピュータすなわち、デジタル処理装置（以下では、コンピュータと呼称する）12が含まれる。所期の実施例の1つでは、コンピュータ12は、図示のように米国ニューヨーク州アーモンクのInternational Business Machines Corporation (IBM) が製造するパーソナル・コンピュータ

とするか、付随するIBM Network Stationを有する、AS 400などの商標の下で販売されるコンピュータを含む、任意のコンピュータとすることができます。または、コンピュータ12は、UNIXコンピュータ、OS/2サーバ、Windows NTサーバー、AIX 3.2.5.が走行する主記憶128MBのIBM RS/6000 250ワークステーション、またはIBM社のラップトップ・コンピュータとすることができます。

【0016】コンピュータ12には、暗号化モジュール14が含まれ、この暗号化モジュール14は、一連のコンピュータ実行可能命令としてコンピュータ12内のプロセッサによって実行することができる。これらの命令は、たとえばコンピュータ12のRAM内に常駐することができる。

【0017】その代わりに、図2に示された、コード要素AないしDを格納されたコンピュータ使用可能媒体15Aを有するコンピュータ・ディスクケット15などのコンピュータ可読媒体を用いるデータ記憶装置に命令を格納することができる。または、命令を、DASDアレ

20 イ、磁気テープ、通常のハード・ディスク装置、電子読み取り専用メモリ、光学記憶装置または他の適当なデータ記憶装置に格納することができる。本発明の実施例では、コンピュータ実行可能命令を、コンパイルされたC++互換コードの複数の行とすることができる。

【0018】実際、本明細書の流れ図には、コンピュータ・プログラム・ソフトウェアで実施された本発明のモジュールの構造が示されている。当業者であれば、これらの流れ図が、本発明に従って機能する、集積回路上の論理回路を含むコンピュータ・プログラム・コード要素の構造を示すものであることを諒解するであろう。明らかに、本発明は、その本質にかかる実施態様において、デジタル処理装置（すなわちコンピュータ）に図示のシーケンスに対応する機能ステップのシーケンスを実行するように指示する形のプログラム・コード要素を実行する機械構成要素によって実施される。

【0019】図1からわかるように、暗号化モジュール14は、放送番組供給源16にアクセスし、実際に放送番組供給源16の構成要素とすることができます。本発明によれば、暗号化モジュール14は、放送番組供給源14によって放送される1つまたは複数の番組の、ケーブル、ワイヤまたは無線の放送手段を介する複数のユーザのビデオ装置18への保護された送信のためにこれらの番組を暗号化するのに使用される、暗号化データを提供する。

【0020】図1には、デジタル・テレビジョン22およびデジタル・ビデオ・カセット・レコーダ（VCR）24を用いて通信することができるビデオ装置20を有する第1の例のユーザが示されている。ビデオ装置20には、セット・トップ・ボックス26が含まれ、デジタル・テレビジョン22、VCR24およびセット

・トップ・ボックス26は、バス28を介して互いに通信する。したがって、最小限、ビデオ装置18にはセット・トップ・ボックス26またはその同等物が含まれる。図示されてはいないが、ビデオ装置20には、Digital Versatile Disk (DVD) プレイヤを含めることができる。所期の実施例の1つでは、バス28は、いわゆる「Firewire」または「IEEE 1394」ディジタル・ビデオ・データ・バスである。本発明では、ユーザのビデオ装置20が家庭内ディジタル・システムであることが意図されているが、本明細書に開示される原理は、アナログの家庭内システムにも適用されることを理解されたい。

【0021】上で述べた構成要素は、通常のディジタル・ビデオ構成要素とすることができるが、セット・トップ・ボックス26には、本発明の新規の非暗号化モジュール30が含まれる。たとえば上で述べたFirewire応用などのいくつかの応用分野では、ディジタル・テレビジョン22やVCR24などの他の構成要素に非暗号化モジュール30を含めることができる。非暗号化モジュール30は、下で説明する論理に従って、暗号化モジュール14からの暗号化データを使用して暗号化された放送番組を非暗号化するという点で、暗号化モジュール14の相補物である。

【0022】本発明によれば、各ユーザのビデオ装置18には、複数の装置鍵が与えられる。装置鍵のそれぞれは、所定のビット・サイズの乱数であり、この好ましい実施例の所定のビット・サイズは、64である。特定のビデオ装置18の装置鍵は、そのそれぞれの非暗号化モジュール30からアクセスでき、システム10で使用される装置鍵全体の集合は、まもなく開示する目的のために、暗号化モジュール14からアクセス可能である。さらに、ライセンシング・エージェンシは、それぞれのビデオ装置18に与えられるそれぞれの装置鍵の部分集合のリストを保存する。

【0023】図3は、システム10の装置鍵全体の集合を表す、2次元の行列32を示す図である。この図では、装置鍵が記号 $S_{i,j}$ によって表され、 i は1からNまでの整数（両端を含む）、 j は1からMまでの整数（両端を含む）である。本発明の原理によれば、「 i 」は、行列32の鍵次元34での位置を示す鍵インデックス変数であり、「 j 」は、行列32の集合次元36での位置を示す集合インデックス変数である。

【0024】さらに、「N」は、鍵の「M」個の集合のそれぞれに含まれる装置鍵「S」の数である。言い換えば、「N」は、鍵次元34のカーディナリティ(cardinality)であり、「M」は、集合次元36のカーディナリティである。図3では、鍵の集合「S」が7つあり（すなわち $M=7$ ）、集合のそれぞれに8つの鍵が含まれる（すなわち $N=8$ ）。しかし、開示を簡潔明瞭にするために図3には56個の鍵だけが示されているが、好

14

ましい実施例では32個の鍵の集合のそれぞれに128個の鍵があることを理解されたい。さらに、これより大きいまたはこれより小さい鍵次元34および集合次元36のカーディナリティの値が、本発明の範囲に含まれることを理解されたい。

【0025】本発明の意図によれば、各ユーザのビデオ装置18には、ライセンシング・エージェンシによって行列32から選択された鍵「S」が割り当てられる。たとえば、第1のユーザのビデオ装置20に、鍵 $S_{1,1}$ 、

10 $S_{1,2}, S_{1,3}, S_{1,4}, S_{1,5}, S_{1,6}$ および $S_{1,7}$ が割り当てられる。どの場合でも、各ユーザのビデオ装置18には、「N」個の装置鍵が割り当てられ、各ビデオ装置18には、鍵インデックス変数「i」ごとに装置鍵「S」が1つだけ割り当てられる。しかし、装置が第i位置のそれについて1つの装置鍵を含まない実施態様は、本発明の範囲内である。どの場合でも、ビデオ装置18は、鍵インデックス次元での同一位置で2つの鍵を知ることはない。多数の装置の装置鍵がオーバーラップする可能性はあるが、ビデオ装置18が、他の装置と正確に同一の装置鍵「S」を有しないことが好ましい。

【0026】ビデオ装置18の装置鍵「S」が割り当てられ、ビデオ装置18が使用されるようになった後に、ディジタル・ビデオ番組を含む番組を、図4に示された論理を使用して放送番組供給源16からさまざまなユーザのビデオ装置18へ保護された状態で送信できる。処理はブロック38から開始され、「N」個のセッション番号「 x 」がランダムに生成される。各セッション番号は長さ「1」を有する。好ましい実施例の1つでは、各セッション番号「 x 」の長さ「1」は、64ビットである。その後、ブロック40で、各セッション番号 x を、 i 番目の装置鍵 $S_{i,j}$ （ $j = 1, \dots, M$ ）ごとに1回ずつ、「M」回暗号化して、セッション番号 x の「M」版を作る。

【0027】ブロック40の結果が、図5に示された行列42である。行列42では、各セッション番号 x の複数の暗号化された版 $E(x, S_{i,j})$ を含むセッション鍵ブロックが定義されている。したがって、少なくともブロック40の論理によって、セッション鍵ブロック・ジェネレータが確立される。当業者であれば、図5に示された行列42のサイズが、図3に示された行列32のサイズと同一であることを諒解できる。

【0028】図4のブロック44に移ると、セッション鍵ブロックが、放送データ・ストリームの暗号化番組の先頭に挿入される。これに関して、図6に、番組の暗号化に使用され、その結果、その番組の非暗号化に使用できるセッション鍵を計算するようにビデオ装置18に指示するための1つの特定のメッセージ46の形式を示す。

【0029】図示された特定のメッセージ46には、メッセージのタイプを識別するメッセージ識別フィールド

48と、それに続く32ビットの更新世代番号フィールド50が含まれる。各ビデオ装置18は、更新世代番号が、特定のビデオ装置18の更新と一致するかどうかを判定し、そうである場合には、ビデオ装置18はそのメッセージを検討する。そうでない場合には、ビデオ装置18はそのメッセージを無視する。下で説明するよう、許可されない装置が存在する場合、システム10は、装置鍵「S」を更新し、更新世代番号は、装置の鍵が更新された回数を表す。

【0030】更新世代番号フィールド50の次に、上で述べたセッション鍵ブロックを含むセッション鍵ブロック・フィールド52がある。暗号化プログラムが、メッセージの本体54を確立する。

【0031】適当な更新世代番号の装置がセッション鍵計算メッセージであるメッセージ46を受信した時には、その非暗号化モジュール30が、図4のブロック56に示された論理を呼び出す。ブロック56では、ビデオ装置18が、セッション鍵ブロックからセッション鍵を非暗号化して、放送番組を非暗号化する。これを行うために、ビデオ装置は、その装置鍵S_{i..}(i=1, ..., N)を使用して、それぞれのi番目のセッション番号x_iを非暗号化する。各ビデオ装置は、たとえばセッション番号のすべてに対してXOR演算を使用することなどによって、非暗号化されたセッション番号のすべてをハッシュして、その後にブロック58で放送中の共通鍵として使用されるセッション鍵を作る。したがって、ビデオ装置18は、同一のセッション鍵を計算するが、異なる装置鍵「S」を使用してそのセッション鍵を得る。

【0032】本発明では、ビデオ装置18のうちの1つが、いわゆる「著作権侵害者」によって取得され、その著作権侵害者が装置鍵と共にビデオ装置のクローンを作成して、望ましくないことに番組を受信し、非暗号化できる1つまたは複数の許可されない装置を作る可能性があることが認識されている。ライセンシング・エージェンシがこのような許可されない装置について学ぶことは可能である。本発明が対処する課題は、許可されない装置が読み取れない放送メッセージを許可された装置に送信することである。これを行うために本発明によって実行される論理を、図7に示す。

【0033】判断ブロック60で、ビデオ装置18が暗号漏洩されたものであるかどうか、すなわち、許可されない装置が存在するかどうかを判定する。存在しない場合、処理は状態62で終了する。この状況の下では、図4に示された論理が番組の放送に使用されると理解される。

【0034】その一方で、ライセンシング・エージェンシが、少なくとも1つのビデオ装置18が暗号漏洩されたものであると判定した時には、エージェンシは、暗号漏洩された装置に割り当てられた装置鍵の部分集合にア

クセし、処理は、判断ブロック60からブロック64に進んで、暗号漏洩された装置に割り当てられた特定の装置鍵S_{i..}が存在する、暗号漏洩された装置の少なくとも1つの鍵位置、たとえば第i鍵位置を識別する。開示を明瞭にするために、下の説明では暗号漏洩された装置の単一の鍵位置だけが選択されると仮定することを理解されたい。しかし、下で説明する原理は、複数の装置鍵位置の選択とそれらの同時処理に適用できる。

【0035】ブロック66に移ると、この論理は、上で述べた原理に従う、i以外のすべてのセッション番号x_{...i..}の、j以外のすべて(暗号漏洩されたビデオ装置18の装置鍵S_{...i..}に対して)の対応する装置鍵S_{...i..,..j..}を用いる暗号化を想定したものである。また、ブロック68では、第iセッション番号x_iが、j以外のすべての装置鍵S_{...i..,..j..}を用いて暗号化される。これによって、暗号化について残された唯一のセッション・ブロック行列要素として、選択された暗号漏洩された装置鍵S_{...i..}が存在する位置のセッション番号が残される。

【0036】したがって、ブロック70で、選択された暗号漏洩されたS_{...i..}を使用してある数字が暗号化されるが、この数字は、第iセッション番号x_iではなく、ダミー番号「y」である。その結果、図8に示されたセッション鍵ブロック72が、ブロック70の後に作られ、図7のブロック74で送信される。図からわかるように、図8のセッション鍵ブロック72は、実質的に図5に示された行列42と同一であり、図4の論理で生成されるが、図8のセッション鍵ブロック72に、ダミー番号「y」を暗号化したものを表すダミー位置76が含まれる点が異なる。

【0037】これで、ビデオ装置18のほとんどが、ブロック64で選択された第i位置を占める暗号漏洩された装置の選択された暗号漏洩された装置鍵S_{...i..}を有すると期待されず、すべてのセッション番号「x」を成功裡に非暗号化し、したがって、セッション鍵を成功裡に計算することが理解される。対照的に、暗号漏洩された装置は、第iセッション番号x_iを非暗号化するのではなく、ダミー番号「y」を非暗号化する。その結果、正しいセッション鍵は、ダミーでないセッション番号x_i、(i=1, ..., N)のすべてを組み合わせることによってのみ決定できるので、暗号漏洩された装置は、正しいセッション鍵を計算できず、したがって、番組を含む付随メッセージを非暗号化することができない。

【0038】特定の選択された暗号漏洩された装置鍵S_{...i..}をたまたま使用し、その結果、暗号漏洩された装置と同様に、正しいセッション鍵を計算できない許可された装置に関しては、許可された装置のどれもが、他の許可された装置と正確に同一の装置鍵の組合せを有しないことを想起されたい。これを念頭において、許可された装置のすべてに有効なセッション鍵が与えられるまで、

上で説明した手順を、暗号漏洩された装置の1つまたは複数の i 以外の装置鍵 S_i, \dots について繰り返す。

【0039】後続の繰り返しを行う際には、新しいセッション鍵ブロックは条件的に作られる。具体的に言うと、既存のセッション鍵が、図7に示された手順の開始の前に存在した鍵である場合に限って、新しいセッション鍵ブロックが付随するメッセージによって、装置が新しいセッション鍵を計算するように指示される。当業者であれば、繰り返しのそれぞの後に、追加の許可された装置が正しいセッション鍵を計算でき、暗号漏洩された装置とそのクローンだけが正しいセッション鍵を有しない状態になるまで、「事情を知らない」装置のプールが徐々に小さくなることを理解するであろう。

【0040】条件付きセッション鍵計算メッセージ78のフォーマットの例を、図10に示す。条件付きセッション鍵計算メッセージ78には、メッセージのタイプを識別するメッセージ識別フィールド80と、その後の認証フィールド82が含まれる。認証フィールド82には、所定のセッション鍵を用いなければ非暗号化できない認証データが含まれる。ビデオ装置18が、認証データの非暗号化の際に所定のコード、たとえば、単語「DEADBEEF」を生成する場合、その装置は条件付きセッション鍵計算メッセージ78を検討する。そうでない場合には、その装置はこのメッセージを無視する。認証フィールド82の次に、図6に関連して上で説明したように使用される更新世代番号フィールド84があり、その後に新規のセッション鍵ブロック・フィールド86がある。

【0041】望むならば、上の手順を使用して、許可された装置と暗号漏洩された装置を区別する鍵位置を複数選択することによって、複数の暗号漏洩された装置を分離することができる。どの場合でも、暗号漏洩された装置を分離した後に、許可された装置の装置鍵を、暗号化鍵として正しいセッション鍵を使用して更新することができる。更新のたびに、上で述べた更新サイクル番号が1つ増やされる。

【0042】図9は、前の段落で述べた論理の詳細を示す図である。処理はブロック88から開始され、共通のセッション鍵（その鍵が有効であるかどうかに無関係に）を有する装置のプールごとに「DO」ループに入る。判断ブロック90では、テスト中のプールに含まれる装置の特定の装置鍵を検討することによって、すべての装置が暗号漏洩された（図では「不正」と表記）装置であるかどうかを判定する。そうである場合には、この論理は、不正装置とこれ以上通信せずに状態92で終了する。そうでない場合には、この論理は判断ブロック94に進んで、テスト中のプールに含まれる装置が「正規」（すなわち許可された装置）と不正の混合であるかどうかを判定する。そうである場合には、前に述べたようにこの論理はブロック96に進んで、図7に示された

処理を使用し、もう1つの暗号漏洩された鍵を使用してダミー変数「y」を暗号化し、図10の条件付きセッション鍵計算メッセージを使用して図8のセッション鍵ブロック72を送るという処理を反復する。その後、この処理は、ブロック88にループ・バックして、ブロック96からもたらされたより少數の装置のプールを使用して、次の反復についてテストを行う。

【0043】その一方で、判断ブロック94で、テスト中のプールに含まれるすべての装置が許可された（「正規」）装置であると判定された場合、この論理は判断ブロック98に進んで、正規の装置だけを有するプールが複数存在するかどうかを判定する。そうである場合には、帯域幅を節約するために、この論理はブロック100に進んで、1つのプールにセッション鍵変更メッセージを送信して、そのセッション鍵を他の「正規」プールのセッション鍵と交換し、これによって、両方のプールの装置鍵を更新する前に両方のプールがセッション鍵を変更する必要をなくす。

【0044】図11は、図10に関連して上で説明した20原理による、メッセージ識別フィールド104と認証フィールド106を含むセッション鍵変更メッセージ102を示す図である。セッション鍵変更メッセージ102には、セッション鍵変更メッセージ102を認証する装置のプールによって使用されるセッション鍵を含む新規鍵フィールド108も含まれる。

【0045】望むならば、ライセンシング・エージェンシは、下で説明するいわゆる「潜伏」攻撃の威力を下げるために、セッション鍵を保持される「正規」プールの独自の装置鍵をまず更新することができる。具体的に言うと、本発明によって認識されるように、著作権侵害者は、第1の暗号漏洩された装置のクローンを大量に作成し、その装置は、クローンを大量に作成されているので比較的簡単に発見できるが、この著作権侵害者が異なる鍵を秘密にされた第2の暗号漏洩された装置を保持し、これによって、第1の暗号漏洩された装置のクローンを更新するための更新された鍵を学習しようとして検出を逃れる可能性がある。したがって、本発明の論理を、図9のブロック100から、潜伏攻撃の疑いがあるかどうかを判定する判断ブロック110に移動することができる。

40 潜伏攻撃の疑いがある場合、この論理はブロック112に進んで、潜伏中の暗号漏洩された装置を分離するために、すべての「正規」プールについて図7の論理を実行する。これは、各プールが、そのプールの装置によって使用されない鍵のための鍵更新データから、余分な鍵更新データを与えられていないことを確認することによって行われる。したがって、潜伏中の装置は、広く配布されたクローン装置のための鍵更新データの一部を学ぶことができなくなる。

【0046】ブロック112から、または潜伏攻撃の疑いがない場合に判断ブロック110から、この論理は、

最終的にブロック114に進み、各「正規」プールの装置の装置鍵を、そのプールのセッション鍵と図12に示された装置鍵更新メッセージ116を使用して更新する。

【0047】図からわかるように、図12の装置鍵更新メッセージ116には、メッセージのタイプを識別するメッセージ識別フィールド118と、その後の、メッセージの残りの暗号化されたバイト数を示す16ビットの通信長フィールド120が含まれる。通信長フィールド120の後には、上で原理を開示した認証フィールド122と更新世代番号フィールド124がある。

【0048】更新世代番号フィールド124の次に、開始鍵フィールド126がある。本発明によれば、開始鍵フィールド126は、最初に更新される装置鍵の「i」および「j」の値を示す。

【0049】次に、装置鍵更新メッセージ116には、更新される鍵ごとに8バイトを含む更新データ・フィールド128が含まれる。更新データのどれかに、特定のビデオ装置18に関連するデータが含まれる場合、そのビデオ装置は、第i位置での更新データと第j位置の以前の装置鍵との連結に対する組合せ関数を計算する。好ましい実施例では、組合せ関数はXORであるが、以前の鍵と更新データの両方を使用する関数であれば、どれでも適しており、本発明の範囲に含まれる。その結果が、特定のビデオ装置18の新しい第i装置鍵である。ライセンシング・エージェンシは、古い装置鍵と更新データの両方を知っているので、ビデオ装置18の新しい装置鍵も知っている。本明細書で認識されているように、ライセンシング・エージェンシに未知の不正装置は、このステップの結果として、すでに知っているもの以外にはなにも学ぶことはない。

【0050】上のメッセージは、他の応用分野に適するようにフォーマットすることができることを理解されたい。特に重要な応用分野が、コピー・プロテクションである。ハリウッド映画などの放送番組は、「コピー不可」または「1回のみコピー可能」と指定される。VCRなどの合法的に動作する装置が、この制限を尊重することが望ましい。本発明は、次のように使用される。正しく動作することが知られている合法的な装置は、上で述べた形で装置鍵を付与される。放送と共に送信されるセッション鍵ブロックは、セット・トップ・ボックスから家庭のシステムの他の構成要素にそのまま渡される。セット・トップ・ボックスは、セッション鍵を使用して映画を暗号化（または再暗号化）し、他の装置は、本発明を使用してそれを非暗号化する。装置鍵を有する合法的な装置だけが、映画を表示または録画することができ、不正コピーは不可能である。

【0051】同様に、合法的な装置の鍵をクローン複製された非合法な記録装置が作られる場合、本発明を使用して、合法的な、クローン複製されたものでない装置だ

けを更新することができる。好ましい実施例では、装置は、Firewireバスによって接続され、本発明は、「copy-once（1回のみコピー可能）」内容が保護される制限認証方法として既知の機能を提供する。この認証方法を使用するビデオ装置18は、ディジタル・ビデオ・カセット・レコーダ（DVC）と一体型ディジタル・ビデオ・カメラである。通常、他のすべての装置は、DVCまたは一体型ディジタル・ビデオ・カメラに接続された時だけこの認証方法を使用する。

【0052】ライセンシング・エージェンシが更新サイクルの実行を希望する時には、すべてのcopy-once放送の前に、更新命令を付加しなければならない。この更新命令は、レコーダが電源を切断され、番組を受信していない場合に備えて、単独の番組のためだけに送信してはならず、数週間にわたって繰り返されなければならない。さらに、1日1回（たとえば午後3時）全更新サイクルの全体の活動記録を放送しなければならない。したがって、長期間電源を切断されていた「リップ・バン・ワインクル」装置を、24時間以内に最新レベルにすることができる。実際、更新活動記録をより頻繁に放送する「更新チャネル」を設けることができる。

【0053】更新の後に、セッション鍵が旧世代である記録された素材は、もはや機能しなくなる。しかし、これは必ずしも望ましくない状態ではない。というのは、「copy-onceモード」の目的が、「タイム・シフト」（別の時に再生するために番組を記録する）用であり、そのような形で記録された映画が長期間存続することは、内容所有者の観点からは望ましくないからである。

【0054】それでも、新しい更新サイクルの先頭で、記録の寿命が短すぎる瞬間が存在する可能性がある。これを考慮に入れるために、ライセンス・エージェンシは、新しい更新サイクルを予想することができ、新しい更新サイクルの直前に、現在の世代のセッション鍵ブロックと、まだ配布されていない次の世代のセッション鍵ブロックの両方を送信することができる。

【0055】「Firewire」バス応用例に加えて、本発明では、本明細書に開示された原理を、衛星システム、ケーブル・テレビジョン・システム、DVDマービー、および、インターネット上または他の放送配布媒体を介する他の広く配布されているマルチメディア内容を含む他の放送応用分野に適用できることが認識されている。

【0056】下に、上で開示した発明を実施するコンピュータ擬似コード・リストイングを示す。

【0057】本明細書で図示され、詳細に説明された特

定の「暗号漏洩された受信装置の存在下で放送番組を暗号化するためのシステム」は、本発明の上述の目的を完全に達成することができるが、これは本発明の好ましい実施例であり、したがって、本発明によって広義に意図される目的を代表するものであり、本発明の範囲は、当

* 業者に明白になるであろう他の実施例を完全に包含し、本発明の範囲は、請求項以外の何物によっても制限されないことを理解されたい。

【0058】

* 【表1】

/*

サイズに関する前提：

以下のルーチンがすでに存在する。これらのルーチンは、このプロトコルの他の動作のために必要である。このサイジングを行う際に使用される具体的な前提を述べる。

*/

```
void *read(); /* バスから読み取り、現在のバッファを返す。このルーチン
   是、データが返されるまでブロックする。バス上のブロックサ
   イズは、最大512バイトである。バッファ管理は、このルー
   チンのトロリにあり、おそらくピンポン・バッファと別のスレッ
   ドが使用される。コマンドがバッファ境界をまたくことはない
   と仮定する。バンド外信号（たとえばバス・リセット）は、全
   く返されない。その代わりに、プロセッサ全体がリセットされ
   る。バッファは、必ずlong *に位置させられる。 */
void hash(unsigned long *from, unsigned long *to, short length);
/* メモリ内の所持の区域をハッシュし、ハッシュをto区域にセッ
   トする。lengthはバイト単位である。 */
void decrypt(unsigned long *from, unsigned long *to, short length,
             unsigned long *key);
/* 所持のバッファを非暗号化する。fromとtoが同一の場合、その
   場所で非暗号化する。lengthはバイト単位である。keyは必ず8バ
   イト（2つのlong）である。非暗号化処理は、一般に、バスに追
   従できる（鍵が頻繁に変更される場合を除く）。 */
```

【表2】

23

24

```

#define ntohl(v) (v)

/* バス上の数値をプロセッサ固有形式に変換する。これによって
、たとえばビッグ・エンディアンがリトル・エンディアンに変換
される。このサイジングでは無効と仮定する。 */

// NVRAM
static unsigned long deviceKeys[32];
static unsigned long globalGeneration;

// ROM; must be different for each device
static const unsigned short keyPosition[33];
/* 装置鍵の各ワード内のセッション鍵に含まれるワード。トリック
: 第33位置は、必ず鍵の总数より大きいので、末尾を超えたかどうか
を検査する必要はない。 */

void calculateSessionKey(
    long sessionKey[2], // ルーチンによって書き込まれる
    unsigned long *buf) // バッファの現在の内容
{
    unsigned long X[32];
    unsigned short word; // バッファの先頭にあるunsigned longの鍵の位置
    short l = 0; // 鍵ワードのインデックス

    unsigned long gen = ntohl(buf[0]);
    gen >>= 8;
}

```

【表3】

25

26

```

for (word = -1; word < 16*256*2 - 2; word += 128) {
    for (; word + 128 > keyPosition[i]; i++) {
        X[i] = ntohs(buf[keyPosition[i] - word]);
    }
    buf = read();
}

if (gen == globalGeneration) {

    sessionKey[0] = sessionKey[1] = 0;

    for (i=0; i < 32; i += 2) {
        unsigned long t[2];
        decrypt(&X[i], t, 8, &deviceKeys[i]);
        sessionKey[0] ^= t[0];
        sessionKey[1] ^= t[1];
    }
}

void newSessionKey(
    long sessionKey[2], // DEADBEEFが見つかった場合にこのループでセッ
    トされる
    unsigned long *buf) // バッファの現在の内容
{

```

【表4】

27

28

```

        decrypt(&buf[1], &buf[1], 16, sessionKey);

        if (buf[1] == 0xDEADBEEF) {
            sessionKey[0] = buf[2];
            sessionKey[1] = buf[3];
        }
    }

void updateDeviceKeys{
    long sessionKey[2], // 現在のセッション鍵、変更されない
    unsigned long *buf) // バッファの現在の内容
{
    unsigned long X[32];
    unsigned short word; // 長さ：現在のバッファを含むunsigned longの数
    short i = 0; // 鍵番号のインデックス

    unsigned long gen = ntohl(buf[0]);
    unsigned long t   = ntohl(buf[1]);
    unsigned long deadBeef;
    unsigned short start = (unsigned short) (t >> 16); // 先頭の鍵番号
    unsigned short len   = (unsigned short) (t); // 鍵の数

    gen >>= 8;

    decrypt(&buf[2], &buf[2], 504, sessionKey);
}

```

【表5】

29

30

```

deadBeef = buf[2];

for (word = start << 1 - 3; ;) {
    for (; word + 128 > keyPosition[i]; i++) {
        if (word <= keyPosition[i]) {
            X[i] = ntohl(buf[keyPosition[i] - word]);
        }
    }
    word += 128;
    if (word >= (start + len) << 1 - 3) {
        break;
    }
    buf = read();
    decrypt(buf, buf, 512, sessionKey);
}

if (deadBeef == 0xDEADBEEF) {

    globalGeneration = gen;

    for (i= start >> 8; i <= (start + len) >> 8; i++) {
        unsigned long t[4];
        short n = keyPosition[i << 1] >> 1;
        if (n < start || n - start >= len) {
            continue;
        }
        for (j = 0; j < 4; j++) {
            t[j] = ntohl(buf[n - start + len - i + j]);
        }
        for (j = 0; j < 4; j++) {
            buf[n - start + len - i + j] = htonl(t[j] ^ X[i]);
        }
    }
}

```

【表6】

```

        }

        t[0] = deviceKeys[i];
        t[1] = deviceKeys[i+1];
        t[2] = X[i];
        t[3] = X[i+1];
        hash(t, &deviceKeys[i], 16);
    }

}

int main(int argc, char *argv[])
{
    return 0;
}

void *read()
{
    return 0;
}

void hash(unsigned long *from, unsigned long *to, short length)
{
}

```

【表7】

```

void decrypt(unsigned long *from, unsigned long *to, short length,
            unsigned long *key)
{
}

```

【0059】まとめとして、本発明の構成に関して以下の事項を開示する。

【0060】(1) 装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵をそれぞれが含む複数のユーザ装置と、セッション鍵ブロックを作るために装置鍵の前記集合を用いて複数のセッション番号を暗号化するための少なくとも1つのセッション鍵ブロック・ジェネレータであって、前記装置のうちの少なくとも1つが暗号漏洩された装置鍵を定義する暗号漏洩された装置であると判定された時に前記セッション番号のうちの少なくとも1つがダミー番号になり、前記ダミー番号が少なくとも1つの暗号漏洩された装置鍵によって暗号化され、前記セッション鍵ブロックが番組の非暗号化に使用するために送信される、前記少なくとも1つのセッション鍵ブロック・ジェネレータと、各ユーザ装置にアクセスでき、前記セッション鍵ブロックおよび前記装置のそれぞれの前記装置鍵に基づいてセッション鍵を判定するために前記装置の前記装置鍵にアクセスする非暗号化モジュールであって、前記セッション鍵が、前記装置が前記セ

ッション鍵の生成に前記ダミー番号を使用しない限り、前記番組を非暗号化するためにユーザ装置によって使用可能である、前記非暗号化モジュールとを含む、1つまたは複数の放送番組を暗号化するためのシステム。

(2) 装置鍵の前記集合が、鍵次元および集合次元を含む少なくとも2次元の行列によって表され、前記鍵次元が、鍵インデックス変数「i」によってそれが表される「N」個の鍵位置を表し、前記集合次元が、集合インデックス変数「j」によってそれが表される

40 「M」個の集合を表し、各装置鍵をS_{1,1}によって表すことができる、上記(1)のシステム。

(3) ある装置の2つの装置鍵のいずれもが、互いに同一の鍵インデックス変数「i」を有しない、上記(2)のシステム。

(4) 各セッション番号をx_{1,1}によって表すことができるよう、鍵インデックス変数「i」ごとにそれぞれのセッション番号が設けられ、各セッション番号x_{1,1}が、前記セッション鍵ブロックを作るために第i鍵次元の装置鍵によってのみ暗号化される、上記(3)のシステム

50

ム。

(5) 暗号漏洩された装置鍵を有しないすべての装置が、少なくとも第1セッション鍵を生成し、暗号漏洩された装置鍵を有するすべての装置が、少なくとも第2セッション鍵を生成し、第1セッション鍵だけが前記番組の非暗号化に有用になるように、各装置が、前記第*i*セッション番号を非暗号化するためにそれぞれの第*i*装置鍵*S_i*を使用する、上記(4)のシステム。

(6) 前記第1セッション鍵を生成する装置が、少なくとも第1プールを定義し、前記第2セッション鍵を生成する装置が、少なくとも第2プールを定義し、前記システムがさらに、前記第1プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に前記第1プール内の前記装置に、前記装置が新しい装置鍵を生成するために操作する更新データを送信するためのコンピュータ可読コード手段を含む、上記(5)のシステム。

(7) 前記第2セッション鍵を生成する装置が、少なくとも第2プールを定義し、前記システムがさらに、前記第2プール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合に前記第2プール内の装置に新しいセッション鍵を生成させるためのコンピュータ可読コード手段を含む、上記(5)のシステム。

(8) 暗号漏洩されない装置の第1集合が、第1プールを定義し、暗号漏洩されない装置の第2集合が、第3プールを定義し、前記第1プールおよび前記第3プールのそれぞれが、暗号漏洩された装置を含まず、前記システムがさらに、前記第1プール内の装置に、そのセッション鍵を前記第3プール内の装置の前記セッション鍵によって置換させるためのコンピュータ可読コード手段を含む、上記(5)のシステム。

(9) ディジタル番組を放送するためにこれを暗号化するためのコンピュータ使用可能コード手段を有するコンピュータ使用可能媒体を含むデータ記憶装置を具備するコンピュータにおいて、前記コンピュータ使用可能コード手段が、*i*が1とNを含む1からNまでの整数であり、*j*が1とMを含む1からMまでの整数であり、

「*i*」が装置鍵*S_i*の行列の鍵次元での位置を示す鍵次元インデックス変数であり、「*j*」が前記行列の集合次元での位置を示す集合インデックス変数であり、

「N」が鍵のM個の集合のそれぞれの装置鍵の個数であるものとして、前記装置鍵*S_i*の行列にアクセスするためのコンピュータ可読コード手段と、鍵インデックス変数「*i*」ごとに各ディジタル・ビデオ装置に1つの装置鍵だけが割り当てられるように、複数の前記ディジタル・ビデオ装置に装置鍵の前記行列からそれぞれの複数の装置鍵を割り当てるためのコンピュータ可読コード手段と、*i*が1とNを含む1からNまでの整数であるものとして、各セッション番号*x_i*がそれぞれの鍵インデッ

クス変数「*i*」に対応するように複数の前記セッション番号*x_i*を生成するためのコンピュータ可読コード手段と、*j*が1とMを含む1からMまでの整数であるものとして、セッション鍵ブロックを生成するために、すべての装置鍵*S_i*を用いて各セッション番号*x_i*を暗号化するためのコンピュータ可読コード手段とを含む、コンピュータ。

(10) 前記ディジタル・ビデオ装置のうちの1つまたは複数が暗号漏洩された装置であるかどうかを判定する

10ためのコンピュータ可読コード手段と、前記暗号漏洩された装置の少なくとも1つの暗号漏洩された装置鍵によって暗号化されるダミー番号として、前記セッション番号のうちの少なくとも1つを作るためのコンピュータ可読コード手段とをさらに含む、上記(9)のコンピュータ。

(11) 第1ディジタル・ビデオ装置が、第1セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第1ディジタル・ビデオ装置が、少なくとも第1プールを定義し、第2デ

20ィジタル・ビデオ装置が、第2セッション鍵を生成するために前記セッション鍵のうちの少なくとも一部を非暗号化し、前記第2ディジタル・ビデオ装置が、少なくとも第2プールを定義し、前記コンピュータがさらに、前記第1プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に前記第1プール内の前記ディジタル・ビデオ装置に、前記ディジタル・ビデオ装置が新しい装置鍵を生成するために操作する更新データを送信するためのコンピュータ可読コード手段を含む、上記(10)のコンピュータ。

30(12) 第2ディジタル・ビデオ装置が、第2セッション鍵を生成するために前記セッション鍵ブロックの少なくとも一部を非暗号化し、前記第2ディジタル・ビデオ装置が、少なくとも第2プールを定義し、前記コンピュータがさらに、前記第2プール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合に前記第2プール内の装置に新しいセッション鍵を生成させるためのコンピュータ可読コード手段を含む、上記(10)のコンピュータ。

(13) 暗号漏洩されない装置の第1集合が、第1プールを定義し、暗号漏洩されない装置の第2集合が、第3プールを定義し、前記第1プールおよび前記第3プールのそれぞれが、暗号漏洩された装置を含まず、前記コンピュータがさらに、前記第1プール内の装置に、そのセッション鍵を前記第3プール内の前記装置の前記セッション鍵によって置換させるためのコンピュータ可読コード手段を含む、上記(10)のコンピュータ。

(14) 前記ディジタル・ビデオ装置と組み合わされた、上記(9)のコンピュータ。

(15) *i*が1とNを含む1からNまでの整数であり、*j*が1とMを含む1からMまでの整数であり、「N」が

鍵のM個の集合のそれぞれの装置鍵の数であるものとして、それが「j」装置鍵 $S_{j,1}$ によって暗号化されるセッション番号 $x_{j,i}$ を含み、少なくとも次元「i」および「j」を有する行列によって表現できるセッション鍵ブロックを受信するためのコンピュータ可読コード手段と、変数「i」ごとに1つだけデジタル・ビデオ装置に割り当てられる複数の局所装置鍵にアクセスするためのコンピュータ可読コード手段と、前記局所装置鍵を使用して前記セッション鍵ブロックからのセッション鍵を非暗号化するためのコンピュータ可読コード手段とを含む、少なくとも1つのデジタル番組を受信し、提示するために構成された前記デジタル・ビデオ装置のための非暗号化モジュール。

(16) さらに、前記デジタル・ビデオ装置が暗号漏洩された装置鍵を有しない場合に、前記デジタル・ビデオ装置が第1セッション鍵を生成し、前記デジタル・ビデオ装置が1つまたは複数の暗号漏洩された装置鍵を有する場合に、前記デジタル・ビデオ装置が第2セッション鍵を生成し、前記第1セッション鍵だけが前記デジタル・ビデオ番組の非暗号化に有用になるよう、第iセッション番号を非暗号化するためにそれぞれの第i局所装置鍵を使用するためのコンピュータ可読コード手段を含む、上記(15)のモジュール。

(17) さらに、更新データを受信するためのコンピュータ可読コード手段を含み、前記モジュールが、1つまたは複数の新しい局所装置鍵を生成するために前記更新データを操作するために1つまたは複数の前記局所装置鍵を使用する、上記(16)のモジュール。

(18) さらに、放送メッセージに応答して、前記セッション鍵を他の装置のセッション鍵によって置換するためのコンピュータ可読コード手段を含む、上記(17)のモジュール。

(19) 装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵を複数のユーザ装置に供給するステップと、セッション鍵ブロックを作るために装置鍵の前記集合を用いて複数のセッション番号を暗号化する少なくとも1つのセッション鍵ブロック・ジェネレータを生成するステップと、前記ユーザ装置のうちの少なくとも1つが、暗号漏洩された装置鍵を定義する暗号漏洩された装置であることが判定された時に、前記セッション番号のうちの少なくとも1つがダミー番号になるように定義するステップと、暗号漏洩された装置鍵を用いて前記ダミー番号を暗号化するステップと、1つまたは複数の放送番組の非暗号化に使用するために前記セッション鍵ブロックを送信するステップと、前記ユーザ装置がセッション鍵の生成に前記ダミー番号を使用しない限り、前記番組を非暗号化するためにユーザ装置によって使用可能な前記セッション鍵を、前記セッション鍵ブロックおよび前記ユーザ装置のそれぞれの前記装置鍵に基づいて判定するために各ユーザ装置の前記装置鍵にアクセスする

ステップとを含む、前記1つまたは複数の放送番組の保護された送信のためのコンピュータ実施される方法。

(20) 装置鍵の前記集合が、鍵次元および集合次元を含む少なくとも2次元の行列によって表現可能であり、前記鍵次元が、鍵インデックス変数「i」によってそれが表される「N」個の鍵位置を表し、前記集合次元が、集合インデックス変数「j」によってそれが表される「M」個の集合を表し、各装置鍵を $S_{j,1}$ によって表すことができるようになっている、上記(19)の方法。

(21) あるユーザ装置の2つの装置鍵のどれもが、互いに同一の鍵インデックス変数「i」を有しない、上記(20)の方法。

(22) 各セッション番号を $x_{j,i}$ によって表すことができるよう、鍵インデックス番号「i」ごとにそれぞれのセッション番号を供給するステップと、前記セッション鍵ブロックを作るために、第i鍵次元の装置鍵だけを用いて各セッション番号 $x_{j,i}$ を暗号化するステップとを含む、上記(21)の方法。

(23) 前記暗号漏洩された装置鍵を有しないすべてのユーザ装置が、少なくとも第1セッション鍵を生成し、前記暗号漏洩された装置鍵を有するすべてのユーザ装置が、少なくとも第2セッション鍵を生成し、前記第1セッション鍵だけが、前記番組の非暗号化に有用になるよう、各ユーザ装置が、第iセッション番号を非暗号化するためにそれぞれの第i装置鍵 $S_{j,1}$ を使用する、上記(22)の方法。

(24) 前記第1セッション鍵を生成するユーザ装置が、少なくとも第1プールを定義し、前記第2セッション鍵を生成するユーザ装置が、少なくとも第2プールを定義し、前記方法がさらに、前記第1プール内のすべてのユーザ装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に、前記第1プール内の前記ユーザ装置に、新しい装置鍵を生成するために前記ユーザ装置が操作する更新データを送信するステップを含む、上記(23)の方法。

(25) 前記第2セッション鍵を生成するユーザ装置が、少なくとも第2プールを定義し、前記方法がさらに、前記第2プール内のすべてのユーザ装置が、暗号漏洩された装置であるかどうかを判定し、そうでない場合に、前記第2プール内のユーザ装置に新しいセッション鍵を生成させるステップを含む、上記(23)の方法。

(26) 暗号漏洩されていない装置の第1集合が、第1プールを定義し、暗号漏洩されていない装置の第2集合が、第3プールを定義し、前記第1プールおよび前記第3プールのそれぞれが、暗号漏洩された装置を含まず、前記方法がさらに、前記第1プール内の装置に、前記第3プール内の前記装置の前記セッション鍵を用いてそれぞれのセッション鍵を置換させるステップを含む、上記(23)の方法。

(27) デジタル処理装置によって読み取ることができるコンピュータ・プログラム記憶装置と、デジタル番組の放送のためにこれを暗号化するための方法ステップを実行するために前記デジタル処理装置によって実行可能な命令を含む、前記プログラム記憶装置上のプログラム手段とを含み、前記方法ステップが、 i が1とNを含む1からNまでの整数であり、 j が1とMを含む1からMまでの整数であり、「 i 」が装置鍵 $S_{i,j}$ の行列の鍵次元での位置を示す鍵インデックス変数であり、

「 j 」が前記行列の集合次元での位置を示す集合インデックス変数であり、「N」が鍵のM個の集合のそれぞれの装置鍵の数であるものとして、前記装置鍵 $S_{i,j}$ の行列にアクセスするステップと、鍵インデックス変数

「 i 」ごとに各デジタル・ビデオ装置に1つの装置鍵だけが割り当てられる形で、複数の前記デジタル・ビデオ装置に、前記装置鍵の行列から複数の装置鍵を割り当てるステップと、 i が1とNを含む1からNまでの整数であるものとして、それぞれが鍵インデックス変数

「 i 」に対応する複数のセッション番号 x_i を生成するステップと、 j が1とMを含む1からMまでの整数であるものとして、セッション鍵ブロックを生成するためには、すべての装置鍵 $S_{i,j}$ を用いて各セッション番号 x_i を暗号化するステップとを含む、コンピュータ・プログラム装置。

(28) 前記方法ステップがさらに、前記デジタル・ビデオ装置のうちの1つまたは複数が暗号漏洩された装置であるかどうかを判定するステップと、前記暗号漏洩された装置の少なくとも1つの暗号漏洩された装置鍵によって暗号化されるダミー番号として、前記セッション番号のうちの少なくとも1つを作るステップとを含む、上記(27)のコンピュータ・プログラム装置。

(29) 第1デジタル・ビデオ装置が、第1セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第1デジタル・ビデオ装置が、少なくとも第1プールを定義し、第2デジタル・ビデオ装置が、第2セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第2デジタル・ビデオ装置が、少なくとも第2プールを定義し、前記方法ステップがさらに、前記第1プール内のすべてのデジタル・ビデオ装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に、新しい装置鍵を生成するために前記第1プール内の前記デジタル・ビデオ装置が操作する更新データを前記第1プール内の前記デジタル・ビデオ装置に送信するステップを含む、上記(28)のコンピュータ・プログラム装置。

(30) 第2デジタル・ビデオ装置が、第2セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第2デジタル・ビデオ装置が、少なくとも第2プールを定義し、前記方

法ステップがさらに、前記第2プール内のすべてのデジタル・ビデオ装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合は、前記第2プール内のデジタル・ビデオ装置に新しいセッション鍵を生成させるステップを含む、上記(28)のコンピュータ・プログラム装置。

(31) 暗号漏洩されない装置の第1集合が、第1プールを定義し、暗号漏洩されない装置の第2集合が、第3プールを定義し、前記第1プールおよび前記第3プール

10 のそれぞれが、暗号漏洩された装置を含まず、前記方法ステップがさらに、前記第1プール内の装置に、前記第3プール内の前記装置のセッション鍵を用いてそのセッション鍵を置換させるステップを含む、上記(28)のコンピュータ・プログラム装置。

(32) 前記デジタル・ビデオ装置と組み合わされた、上記(27)のコンピュータ・プログラム装置。

(33) デジタル処理装置によって読み取ることができるコンピュータ・プログラム記憶装置と、デジタル・ビデオ装置に少なくとも1つのデジタル番組を受信

20 させ、提示させるための方法ステップを実行するために前記デジタル処理装置によって実行可能な命令を含む、前記コンピュータ・プログラム記憶装置上のプログラム手段とを含み、前記方法ステップが、 i が1とNを含む1からNまでの整数であり、 j が1とMを含む1からMまでの整数であり、「N」が鍵のM個の集合のそれぞれの装置鍵の数であるものとして、各セッション番号 x_i が第 j 装置鍵 $S_{i,j}$ によって暗号化される暗号化されたセッション番号 x_i を含む、少なくとも次元「 i 」および「 j 」を有する行列によって表すことのできるセッション鍵ブロックを受信するステップと、前記デジタル・ビデオ装置に変数「 i 」ごとに1つだけ割り当てる複数の局所装置鍵にアクセスするステップと、前記局所装置鍵を使用して前記セッション鍵ブロックからのセッション鍵を非暗号化するステップとを含む、コンピュータ・プログラム装置。

30 (34) 前記方法ステップがさらに、前記デジタル・ビデオ装置が暗号漏洩された装置鍵を有しない場合には、前記デジタル・ビデオ装置が第1セッション鍵を生成し、前記デジタル・ビデオ装置が1つまたは複数の暗号漏洩された装置鍵を有する場合には、前記デジタル・ビデオ装置が第2セッション鍵を生成し、前記第1セッション鍵だけが前記デジタル番組の非暗号化に有用になるように、第 i セッション番号を非暗号化するためにそれぞれの第 i 局所装置鍵を使用するステップを含む、上記(33)のコンピュータ・プログラム装置。

(35) 前記方法ステップがさらに、更新データを受信するステップと、1つまたは複数の新しい局所装置鍵を生成するために、前記更新データを操作するのに1つまたは複数の前記局所装置鍵を使用するステップとを含む、上記(34)のコンピュータ・プログラム装置。

50 (36) 前記方法ステップがさらに、更新データを受信するステップと、1つまたは複数の新しい局所装置鍵を生成するために、前記更新データを操作するのに1つまたは複数の前記局所装置鍵を使用するステップとを含む、上記(34)のコンピュータ・プログラム装置。

(36) 前記方法ステップがさらに、放送メッセージに応答して、前記セッション鍵を他の装置のセッション鍵によって置換するステップを含む、上記(35)のコンピュータ・プログラム装置。

【図面の簡単な説明】

【図1】本発明の放送暗号化システムのブロック図である。

【図2】コンピュータ・プログラム製品の概略図である。

【図3】装置鍵行列を示す図である。

【図4】放送番組の後続の非暗号化に使用するためにセッション鍵を暗号化し、ユーザ装置に送信し、非暗号化するための論理の流れ図である。

【図5】セッション鍵ブロックを示す図である。

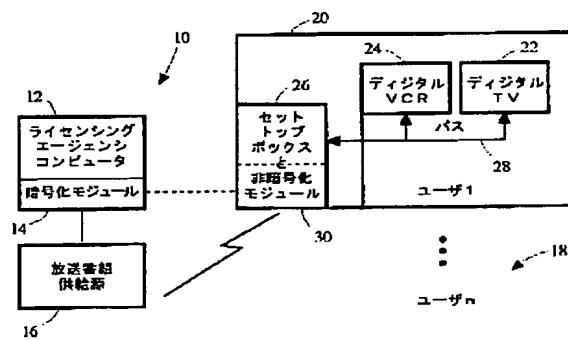
【図6】セッション鍵計算メッセージを示す図である。

【図7】許可されない装置によって保持されていることが既知の少なくとも1つの装置鍵を使用する所定のダミー・セッション番号の暗号化のための論理の流れ図である。

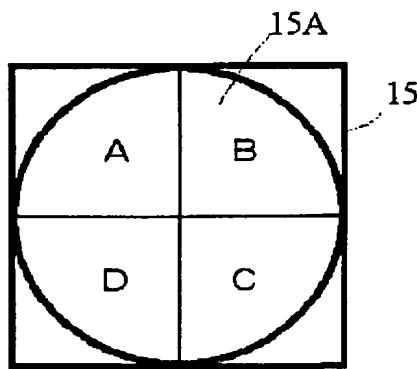
【図8】図7の論理によって生成されるセッション鍵ブロックを示す図である。

【図9】装置のさまざまなプールを処理するために実行

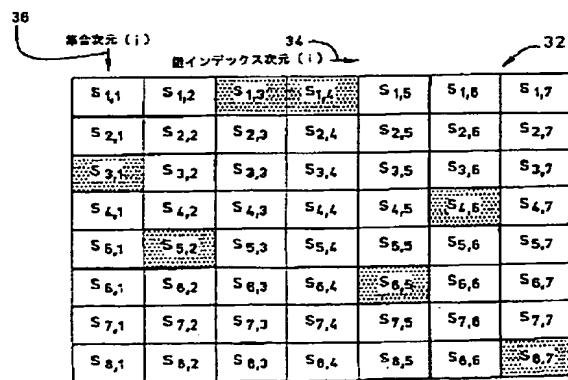
【図1】



【図2】



【図3】

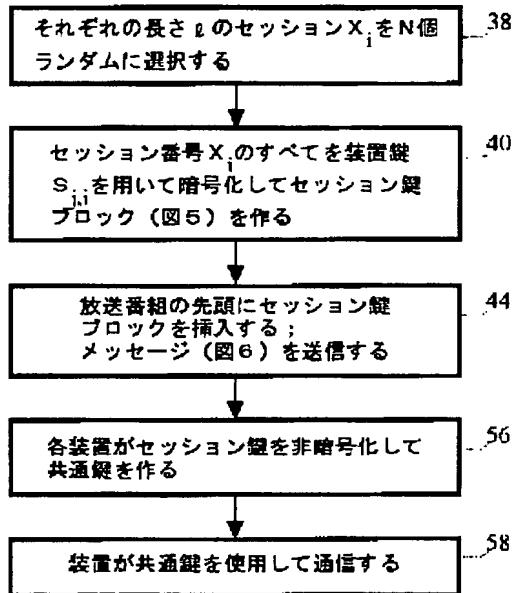


【図5】

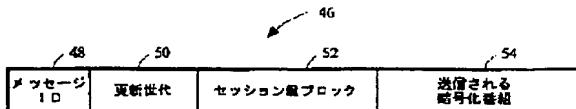
Figure 5 shows a 8x7 session key matrix table. The columns are labeled '42' and the rows are labeled 'E(x_i, S_j)'. The matrix contains elements labeled E(x_i, S_j). The matrix is labeled '36' at the top left.

E(x ₁ , S _{1,1})	E(x ₂ , S _{1,2})	E(x ₃ , S _{1,3})	E(x ₄ , S _{1,4})	E(x ₅ , S _{1,5})	E(x ₆ , S _{1,6})	E(x ₇ , S _{1,7})
E(x ₁ , S _{2,1})	E(x ₂ , S _{2,2})	E(x ₃ , S _{2,3})	E(x ₄ , S _{2,4})	E(x ₅ , S _{2,5})	E(x ₆ , S _{2,6})	E(x ₇ , S _{2,7})
E(x ₁ , S _{3,1})	E(x ₂ , S _{3,2})	E(x ₃ , S _{3,3})	E(x ₄ , S _{3,4})	E(x ₅ , S _{3,5})	E(x ₆ , S _{3,6})	E(x ₇ , S _{3,7})
E(x ₁ , S _{4,1})	E(x ₂ , S _{4,2})	E(x ₃ , S _{4,3})	E(x ₄ , S _{4,4})	E(x ₅ , S _{4,5})	E(x ₆ , S _{4,6})	E(x ₇ , S _{4,7})
E(x ₁ , S _{5,1})	E(x ₂ , S _{5,2})	E(x ₃ , S _{5,3})	E(x ₄ , S _{5,4})	E(x ₅ , S _{5,5})	E(x ₆ , S _{5,6})	E(x ₇ , S _{5,7})
E(x ₁ , S _{6,1})	E(x ₂ , S _{6,2})	E(x ₃ , S _{6,3})	E(x ₄ , S _{6,4})	E(x ₅ , S _{6,5})	E(x ₆ , S _{6,6})	E(x ₇ , S _{6,7})
E(x ₁ , S _{7,1})	E(x ₂ , S _{7,2})	E(x ₃ , S _{7,3})	E(x ₄ , S _{7,4})	E(x ₅ , S _{7,5})	E(x ₆ , S _{7,6})	E(x ₇ , S _{7,7})
E(x ₁ , S _{8,1})	E(x ₂ , S _{8,2})	E(x ₃ , S _{8,3})	E(x ₄ , S _{8,4})	E(x ₅ , S _{8,5})	E(x ₆ , S _{8,6})	E(x ₇ , S _{8,7})

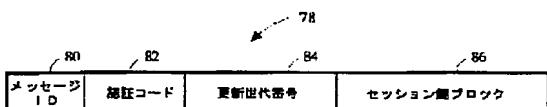
【図4】



【図6】

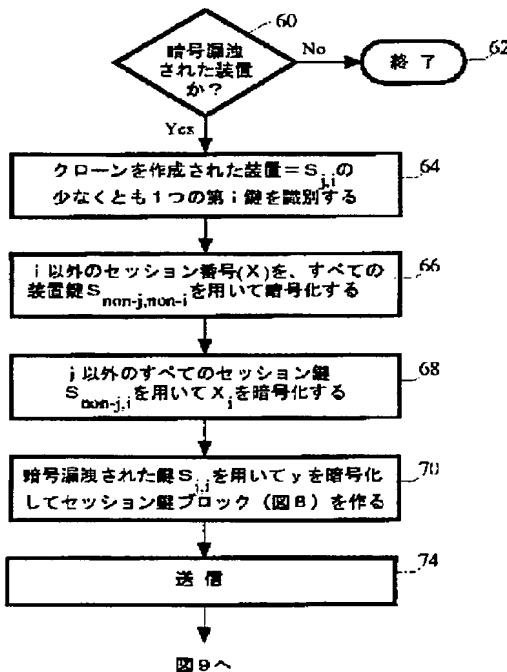


【図10】

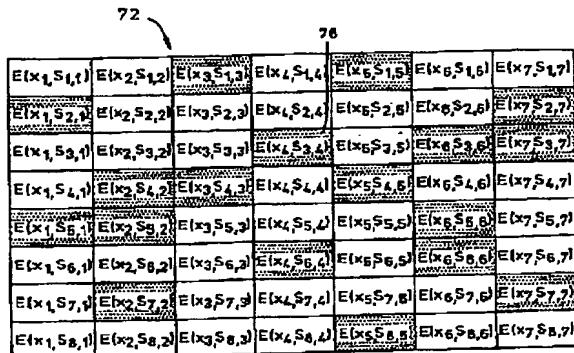


条件付きセッション鍵計算メッセージ

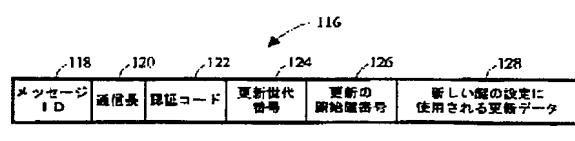
【図7】



【図8】

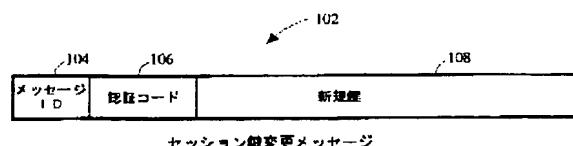


【図12】



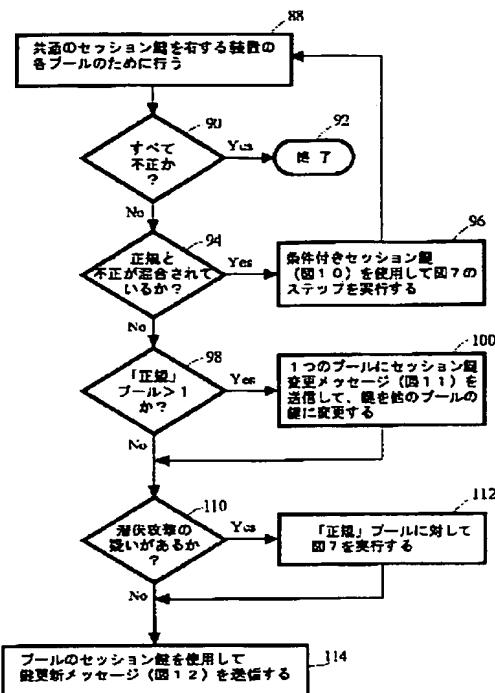
装置鍵更新メッセージ

【図11】



セッション鍵変更メッセージ

【図9】



フロントページの続き

(72)発明者 ケヴィン・スノウ・マカーレイ
 アメリカ合衆国95120 カリフォルニア州
 サンノゼ タナヒル・ドライブ 6721

This Page Blank (uspto)